Responsible Office: Office of the Chief Information Officer

SUBJECT: Minimum Information Technology Security Requirements for LaRCNET

1. REFERENCES

a. NPD 2810.1, "Security of Information Technology."

b. NPR 2810.1, "Security of Information Technology."

c. LAPD 2810.1, "Appropriate Use of NASA Langley Research Center (LaRC) Information Technology Resources."

d. NASA-STD-2804, Minimum Office Automation Software Suite Interface Standards and Product Standards.

2. SUMMARY

a. This directive sets forth NASA Langley Research Center (LaRC) policy and responsibilities for the minimum Information Technology (IT) security requirements to protect the integrity, availability and confidentiality of LaRC IT resources. Noncompliance with this LAPD may result in loss of access to LaRC IT resources.

b. Ultimately all NASA and contractor employees are individually responsible and accountable for the protection of LaRC owned IT resources. We are also collectively responsible for protecting the public's confidence and financial investment in NASA.

3. POLICY

It is the policy of LaRC to:

a. Comply with prescribing NASA and Federal regulations on IT security to ensure adequate protective measures, risk assessments, and IT security plans are in place for all IT resources.

b. Ensure that all IT resources connected to LaRC's internal computer network (LaRCNET) meet minimal IT security standards as defined by the Center Information Technology Security Manager (CITSM) to include, but not be limited to:

(1) Displaying the Chief Information Officer (CIO) Warning Banner.

(2) Installing IT security patches in an expeditious manner.

(3) Restricting access to the resource to the greatest extent possible, to include the use of TCP wrapper software on UNIX systems.

(4) Restricting unnecessary file sharing to the maximum extent possible.

(5) Disabling network services that are not utilized from automatic start-up.

(6) Performing regular, periodic back-ups and verifying their restorability.

(7) Encouraging the selection of good passwords.

(8) Reviewing system logs periodically (weekly at a minimum) for unauthorized access.

(9) Maintaining current anti-virus software (for Macintosh and personal computers) that is configured for the automatic downloading of the latest virus definition files and scanning of all files when they are opened.

c. Prohibit the following activities, without the explicit written permission of the CITSM:

(1) Connecting non-LaRC owned computers to LaRCNET, except for computers owned and operated by LaRC contractors in support of LaRC work.

(2) Connecting any computer on LaRCNET, without proper authorization, to any external network through a direct physical link or a modem, except for those systems that comprise the Langley Remote Access (LaRA) system.

(3) Running programs to analyze network traffic, except in support of the maintenance or security of LaRCNET.

(4) Connecting any IT resource to LaRCNET without ensuring that it meets the minimal IT security standards.

(5) Downloading and installing freeware, shareware, or any other public domain software and/or commercial software from any foreign site, bulletin board, university, Internet Service Provider, or any other non-commercial site.

d. Report all suspected IT security incidents to the CITSM or his/her designee by telephone and not by e-mail.

e. Download and install software if and only if the software has been evaluated for correctness of execution and is available from a NASA or reputable commercial vendor site within the United States.

4. APPLICABILITY

This LAPD applies to all LaRC employees, to all LaRC contractor and subcontractor employees, and to all other individuals authorized access to any LaRC IT resources with authentication requirements.

5. RESPONSIBILITIES

Specific responsibilities of individuals and organizations with regard to the minimum IT security requirements for LaRC IT resources are as follows:

a. LaRC Chief Information Officer

(1) Ensure that LaRC IT policies are enforced to provide secure operation and protection of LaRC systems and information.

(2) Resolve disputes between the CITSM and supervisors with regard to corrective or preventative actions arising from an IT security incident or the preparation of an IT Security Plan.

b. LaRC Center Information Technology Security Manager

(1) Direct LaRCNET personnel to enforce Center IT security policies and guidelines.

(2) Maintain an effective IT security awareness program to include training, briefings, and general IT security information articles or notices to the Center.

c. Network and Computer Services Branch (NCSB)

Terminate LaRCNET connections as directed in response to IT security incidents or violations, when other corrective action is not feasible or was shown to be ineffective.

d. Supervisors

(1) Implement LaRC's policies to manage IT resources.

(2) Ensure that all IT resources under their management control are:

(a) Administered to provide minimum IT security.

(b) Scanned regularly for system vulnerabilities.

(3) Ensure that only users with a need to access the IT resources have current accounts.

(4) Ensure that Foreign Nationals or Foreign Representatives are not given accounts except as permitted by NASA and LaRC policy.

(5) Ensure that information and software are erased from IT resources before excess, transfer, trade-in or disposal in accordance with NASA policy.

(6) Develop an IT Security Plan and Contingency Plan for each system or major application under their management control.

e. Employees

Notify supervisor, system administrators, or the CITSM immediately about any IT security incidents

f. Contracting Officer's Technical Representative

Ensure the proper administration of IT resources connected to LaRCNET that are used by contractor personnel.

6. RECISION

LAPD 2810.1, dated January 13, 2000

Jeremiah F. Creedon
Director